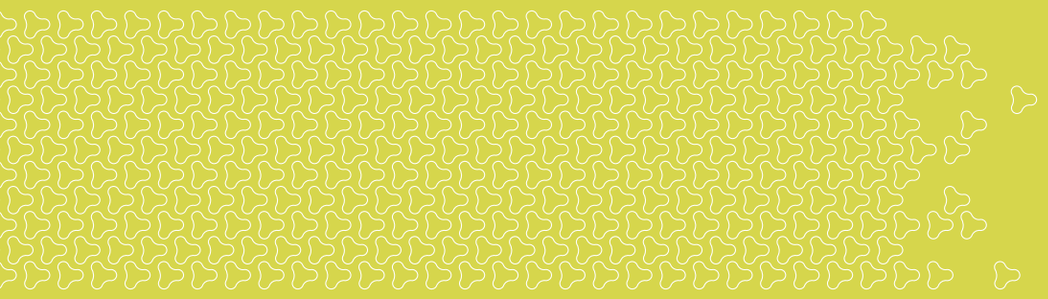
Symantec™

Securing Cloud Applications & Services

AN EXECUTIVE GUIDE

Eric Andrews
Gerry Grealish
Rehan Jalil



> **The ideal Elastic Enterprise, where companies can adapt to achieve the business agility, collaborative capabilities and cost efficiencies needed to effectively compete in today's market, requires an elastic security model that moves with the data, the user, and the application.**
>
> – Rehan Jalil
> SVP of Cloud Security, Symantec

Securing Cloud Applications & Services

AN EXECUTIVE GUIDE

Eric Andrews
Gerry Grealish
Rehan Jalil

The cloud empowers organizations to be more agile, collaborative, and cost-efficient, but benefits of the cloud come with security challenges. How do you gain visibility into what cloud apps people are using and if they are safe? How do you ensure sensitive documents are not being shared inappropriately? How do you adhere to critical compliance regulations? How do you protect against malicious activity? This book addresses all of these questions so you can be safe and secure in the cloud.

TABLE OF CONTENTS
CLICK TO NAVIGATE

2 INTRODUCTION — A FUTURE IN THE CLOUD
3 Migration to the Cloud Office
5 Rethinking the Security Stack for the Cloud
6 Cloud Access Security Brokers (CASBs) —A New Solution for Cloud App Security

10 CHAPTER ONE — CLOUD APP DISCOVERY & ANALYSIS
12 Discovering Cloud Apps
12 Rating and Analysis of Discovered Apps
15 Continuous Monitoring and Reporting

16 CHAPTER TWO — DATA GOVERNANCE & PROTECTION
18 Evolving Role of DLP
18 Data Classification
19 Policy Enforcement
20 Encryption and Tokenization

22 CHAPTER THREE — THREAT DETECTION & INCIDENT RESPONSE
24 The Evolving Role of IDS/IPS
24 Deep Visibility of Cloud Activity
25 Cloud Threat and Anomaly Detection
28 Malware Detection
28 Continuous Monitoring and Incident Analysis

30 CHAPTER FOUR — COMPLIANCE & DATA PRIVACY
32 Baseline Security Certifications
32 Data Use Restrictions
34 Secure and Monitor Regulated Data
34 Protect Regulated Data with Tokenization or Encryption
34 Limit Access to Regulated Data
35 Monitor and Log Interactions with Regulated Data

36 CHAPTER FIVE — SELECTING A CASB SOLUTION

a future in the cloud

Introduction

Migration to the Cloud Office

Enterprises are experiencing a fundamental shift in the way their employees and customers consume technology. The influx of personally owned devices, ubiquitous high-speed internet connectivity and cloud-based applications is redefining the enterprise network. This transformation is happening in nearly every vertical and region, and it is sometimes referred to as a dissolving network perimeter, but in reality, it is an expansion of the traditional enterprise network through mobility and cloud applications. The traditional IT infrastructure that enterprises have built is being extended as companies embrace cloud applications such as Office 365, Google Drive, Box, Dropbox Amazon Web Services, Oracle, and Salesforce. **This shift of workloads into the cloud is rapidly redefining enterprise IT, and offers significant opportunities to enterprises.**

The traditional IT infrastructure that enterprises have built is being extended as companies embrace cloud applications such as Office 365, Google Drive, Box, Dropbox, Amazon Web Services, Oracle, and Salesforce.

COLLABORATION

Cloud apps and services streamline collaboration among users regardless of their platform (e.g., mobile vs. desktop, Windows vs. MAC) or their location.

AGILITY

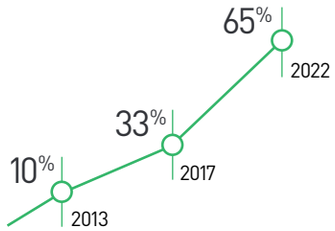
People can be productive immediately upon signing up for cloud services vs. waiting months to procure, install, and customize software. New feature updates are much more frequent as well, as the cloud model helps vendors streamline maintaining their software.

ECONOMICS

The subscription-based model eliminates capital costs and enables a flexible *pay as you go* model for scaling services. Cloud apps also eliminate operational costs, freeing up IT resources and allowing organizations to focus on their core competencies.

CHOICES

Cloud apps are growing at a tremendous rate, and generally offer more competitive options to on-premises software. Furthermore, organizations can try different services and select the appropriate one for their environment, without a huge commitment in time and money.

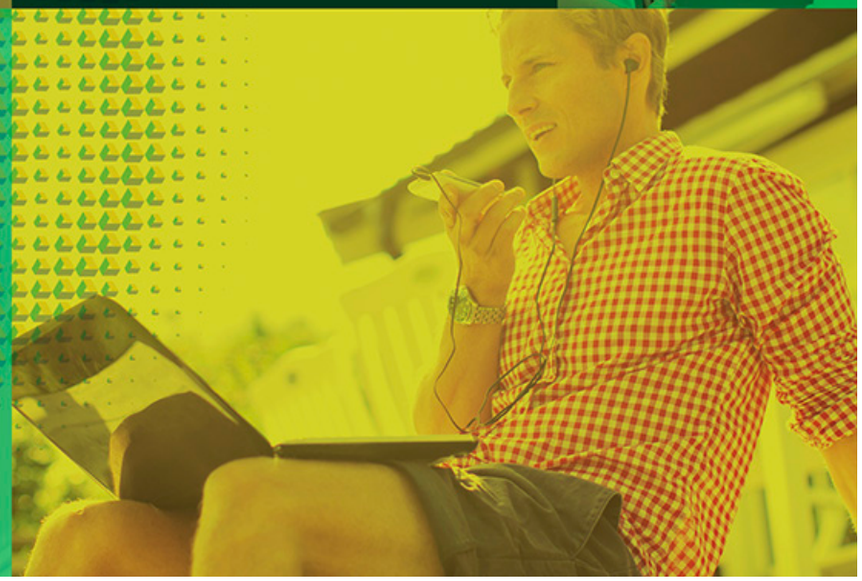


Emerging Cloud Office

Email, Chat, File Sharing, Conferencing, Social, Office Apps. Estimates by Gartner, 2015.

While the expansion into the cloud has many benefits, security and data privacy professionals are being challenged to provide security and governance for cloud applications. Many CISOs lie awake at night wondering: Are sensitive documents being shared inappropriately? How do I ensure malicious users are not hacking into my cloud apps? Which apps should I trust with business-critical information? Are we adhering to critical internal and external compliance regulations?

Similar to the advent of other major information technologies such as email or the web, the rampant adoption of cloud apps and services is driving the need for a new class of security solution to help organizations protect their data that sits inside cloud applications.



The Expanding Enterprise Network

The network perimeter that many traditional security technologies such as the firewall were designed to defend has been punched full of holes to facilitate access to third-party cloud apps and services by remote employees, customers, and suppliers. And in this new world of ubiquitous cloud access, organizations are putting a growing share of their business-critical data in the cloud, which is increasing the volume of traffic and business data flowing between employees to the internet. There is no longer an inside or outside of the network; the cloud has become every organization's *de facto* extended enterprise. In this new reality, security must follow the data, follow the application, and follow the user.

There is no longer an inside or outside of the network; the cloud has become every organization's *de facto* extended enterprise.

Rethinking the Security Stack for the Cloud

The layers of security technology that have traditionally been deployed in the enterprise have a blind spot with regards to the cloud. For example, enterprise next-generation firewalls, intrusion detection and intrusion prevention systems (IDS/IPS), vulnerability scanning, network forensics, security information and event management (SIEM), and data loss prevention (DLP) systems were designed to protect assets that are owned and operated by the IT organization. In general, these systems were not designed to protect corporate data transferred to third-party solutions hosted outside the enterprise and accessible by users anywhere. The need for these traditional security functions hasn't gone away, but a new implementation model suitable to protect sensitive data in the cloud environment is required.

Cloud Access Security Brokers (CASB)

A New Solution for Cloud App Security

In this book we explore the security challenges posed by the use of cloud apps and services and the new cloud security technology that addresses these challenges, known as Cloud Access Security Broker (CASB) solutions.

These new CASB solutions are designed to help organizations enable the productivity gains offered by cloud apps and services by providing critical visibility and control of how these services are being used. They help information security teams:

1. **Identify and evaluate all the cloud apps in use (Shadow IT)**
2. **Enforce cloud application management policies in existing web proxies or firewalls**
3. **Enforce granular policies to govern handling of sensitive information, including compliance-related content**
4. **Encrypt or tokenize sensitive content to enforce privacy and security**
5. **Detect and block unusual account behavior indicative of malicious activity**
6. **Integrate cloud visibility and controls with your existing security solutions**

What is Shadow IT?

The term Shadow IT refers to investment in third-party IT solutions, including cloud apps and services, without oversight from the IT organization. Cloud apps are a big contributor to Shadow IT, as employees or lines of business can easily onboard these services directly and they immediately improve productivity.

SaaS has the greatest variety of services and the fastest growing market.

Cloud Service Models

When migrating workloads to the cloud, there are three basic types of services that organizations may adopt:

IaaS

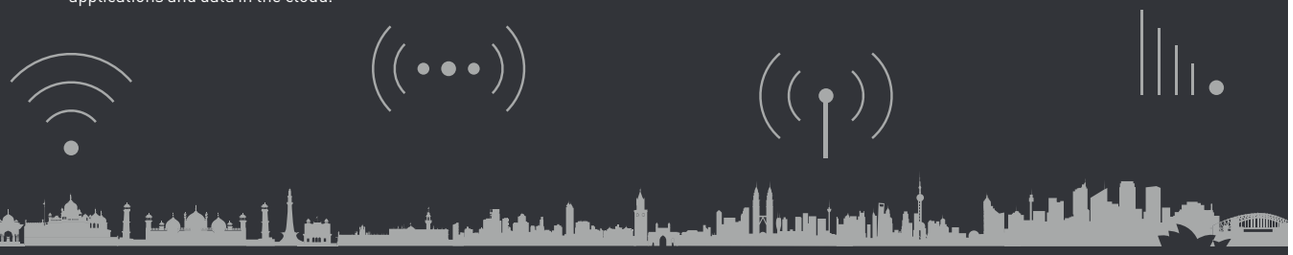
INFRASTRUCTURE AS A SERVICE
Examples include: AWS and Azure. The IaaS provider hosts hardware, software, servers, storage, and other infrastructure components enabling organizations to deploy their own applications and data in the cloud.

PaaS

PLATFORM AS A SERVICE
Examples include: Salesforce's Heroku and AWS' Beanstalk. The PaaS provider delivers both hardware and software tools, typically to support application development.

SaaS

SOFTWARE AS A SERVICE
Examples include: Office 365, Salesforce, and Box. The SaaS provider hosts software applications and makes them available via subscription over the network.



Fundamentals of an effective CASB solution

CASB solutions are often deployed in the cloud as a service, but may also be deployed on-premises in conjunction with your web proxies or as a standalone solution. Effective CASB solutions need to cover a wide range of scenarios, including sanctioned and unsanctioned apps, business and personal accounts on sanctioned apps, mobile devices and desktops, and managed and unmanaged devices. To address all of these scenarios, comprehensive CASB solutions leverage the following:

APIs — Many of the major cloud apps have well-defined APIs that can be leveraged for monitoring activity, analyzing content, and modifying settings as needed.

GATEWAYS — Sitting between the users and their cloud apps, a gateway can provide valuable insights into cloud activity and provide a vehicle for real-time policy enforcement.

LOG DATA — Existing security devices, such as firewalls or secure web gateways, have log data that can be used to help analyze Shadow IT.

AGENTS — Endpoint agents offer another option to manage cloud activity and enforce policies.

The following chapters explore four fundamental areas of an effective CASB solution.

We conclude with a final chapter that examines criteria to consider when evaluating CASB solutions.

CLOUD APP DISCOVERY AND ANALYSIS

Provide Shadow IT discovery and risk analysis, including detailed cloud app ratings, usage analytics, and continuous reporting.

1

DATA GOVERNANCE AND PROTECTION

Provide the ability to enforce data-centric security policies to prevent unwanted activity, such as inappropriate sharing of content. Support encryption and tokenization of compliance-related data.

2

THREAT PROTECTION AND INCIDENT RESPONSE

Prevent malicious activity such as data exfiltration due to account takeover, session hijacking, or insider activity through continuous monitoring of user behavior. Identify and block malware being uploaded or shared within cloud apps and provide tools for incident response.

3

COMPLIANCE AND DATA PRIVACY

Assist with data residency and compliance with regulations and standards, as well as identify cloud usage and the risks of specific cloud services.

4

Find, rate, and compare apps. Decide which to sanction, which to monitor, and which to block.

AUDIT

Sanctioned Apps

Unsanctioned Apps

Company Accounts

SECURED THROUGH GATEWAY AND APP APIs

****
****
BUSINESS LOGIN

****
****
PERSONAL LOGIN

Personal Accounts

SECURED THROUGH GATEWAY

Apps to Monitor

SECURED THROUGH GATEWAY

Apps to Block

FINE TUNE WEB PROXIES AND FIREWALLS; BLOCK APPS

API

Cloud Apps

Gateway

CASB Solution

Logs

Web Proxy / FW

Agent

1

cloud app discovery & analysis

Chapter One

Many organizations are actively embracing select business-ready cloud apps as a strategic part of their IT infrastructure. At the same time, however, their employees are adopting additional *ad hoc* cloud services to aid business productivity or for personal applications, without IT sanction or oversight. This movement toward employee-adopted devices, apps, and cloud services is known collectively as Shadow IT.

Shadow IT exposes an organization to risk by creating a blind spot for CIOs and CISOs.

Do the Shadow IT applications have appropriate security controls?

Do they align with compliance requirements?

Can they operate as conduits for data exfiltration?

As organizations determine their cloud security strategy, visibility is generally their first priority. While traditional network security tools such as web proxies, firewalls or DNS logs provide some basic insights, a comprehensive CASB solution provides much deeper visibility and can reveal detailed analyses on the over 10,000+ apps that permeate the landscape.

Why do organizations require visibility and analysis of their cloud apps?

DISCOVER SHADOW IT

CIOs may want to get a baseline understanding of what cloud apps are being used in their organizations and who is using them.

IDENTIFY RISKY APPS

Security administrators may want to identify SaaS applications that can pose a risk to their environments. For example, understanding which apps have lax security controls, which can be conduits for data exfiltration, or which are hosted in rogue states.

ENSURE COMPLIANCE

Compliance officers may want to continuously monitor apps being used by the organization and individual departments to make sure apps have the appropriate certifications and meet compliance requirements.

IDENTIFY INEFFICIENCIES

Organizations may be concerned that there are many disparate groups using a plethora of cloud applications that provide similar functionality. By identifying all the apps in use and consolidating, they can trim costs and simplify management.

BLOCK RISKY APPS

Security administrators may want to enforce policies that prevent the riskiest apps from being used by their organizations.

SANCTION APPS

Organizations may want to examine current cloud app usage along with cloud app risk analysis to select sanctioned apps to be used by their employees.

SHADOW IT RISK ASSESSMENT

Regardless of what an organization's policy is towards cloud services, performing a Shadow IT audit and risk assessment is essential. In the absence of such an assessment, organizations will not know what applications are running in their environment and what risk they pose.

Discovering Cloud Apps

Research shows the average organization has over 800 cloud apps, the vast majority of which are not *business ready*. This average number has continued to increase over the past two years[1]. Most organizations underestimate this reality by 80–90%.

To get a clearer picture of the current environment, the first step most organizations take is to perform a Shadow IT risk assessment.

This can be done by leveraging log data from existing network devices, like web proxies or firewalls. What organizations are likely to find is the bulk of the usage comes from popular consumer apps, such as Twitter, YouTube, and LinkedIn, along with mainstream collaboration apps such as Office 365, Google Drive, Box, and Dropbox. The long tail of the list often contains obscure apps that could pose a risk to the organization, thus additional analysis is critical.

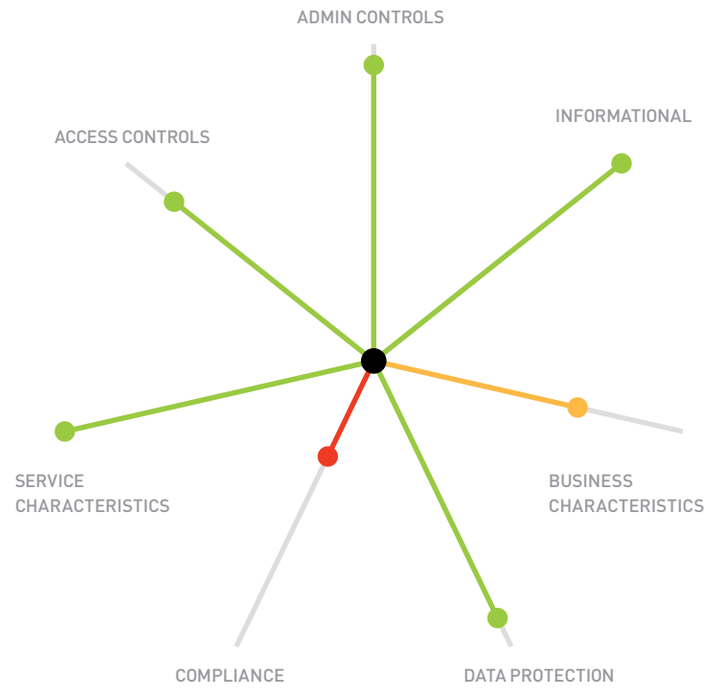
Rating and Analysis of Discovered Apps

To determine the business readiness of discovered apps, organizations need to know if the apps are appropriate for use given the company's security policies, compliance policies, or other corporate requirements. With these insights, organizations can make informed decisions about which apps to sanction, which to allow and monitor, and which to block altogether.

What organizations are likely to find is the bulk of the usage comes from popular consumer apps, such as Twitter, YouTube, and LinkedIn, along with mainstream collaboration apps such as Office 365, Google Drive, Box, and Dropbox.

[1]2H 2015 Elastica Shadow Data Report

Business readiness characteristics of cloud apps can be evaluated across seven dimensions with a comprehensive CASB solution. →



By honing in on the riskiest apps identified in the organization, IT admins can reduce the overall risk exposure for the company. This requires additional usage analysis to identify:

Who is accessing the riskiest apps?

How often are employees accessing these apps?

How much bandwidth is being consumed by these apps?

Which departments are driving this usage?

Which locations are involved?

Which browsers and platforms are employees using?

With this additional layer of insight, IT organizations can formulate strategies to reduce risk, such as coaching individual users or departments to find alternative apps or enforcing policies to restrict access to the riskiest apps.

ACCESS CONTROLS
Does the SaaS service support strong password management controls, federated identity management, multi-factor authentication and integration with enterprise identity solutions such as LDAP and Active Directory?

SERVICE CHARACTERISTICS
Does the SaaS service employ a multi-tenant or a single-tenant architecture, and what policies are in place to address issues associated with multi-tenancy, including data cross pollination between customers and data retention rules?

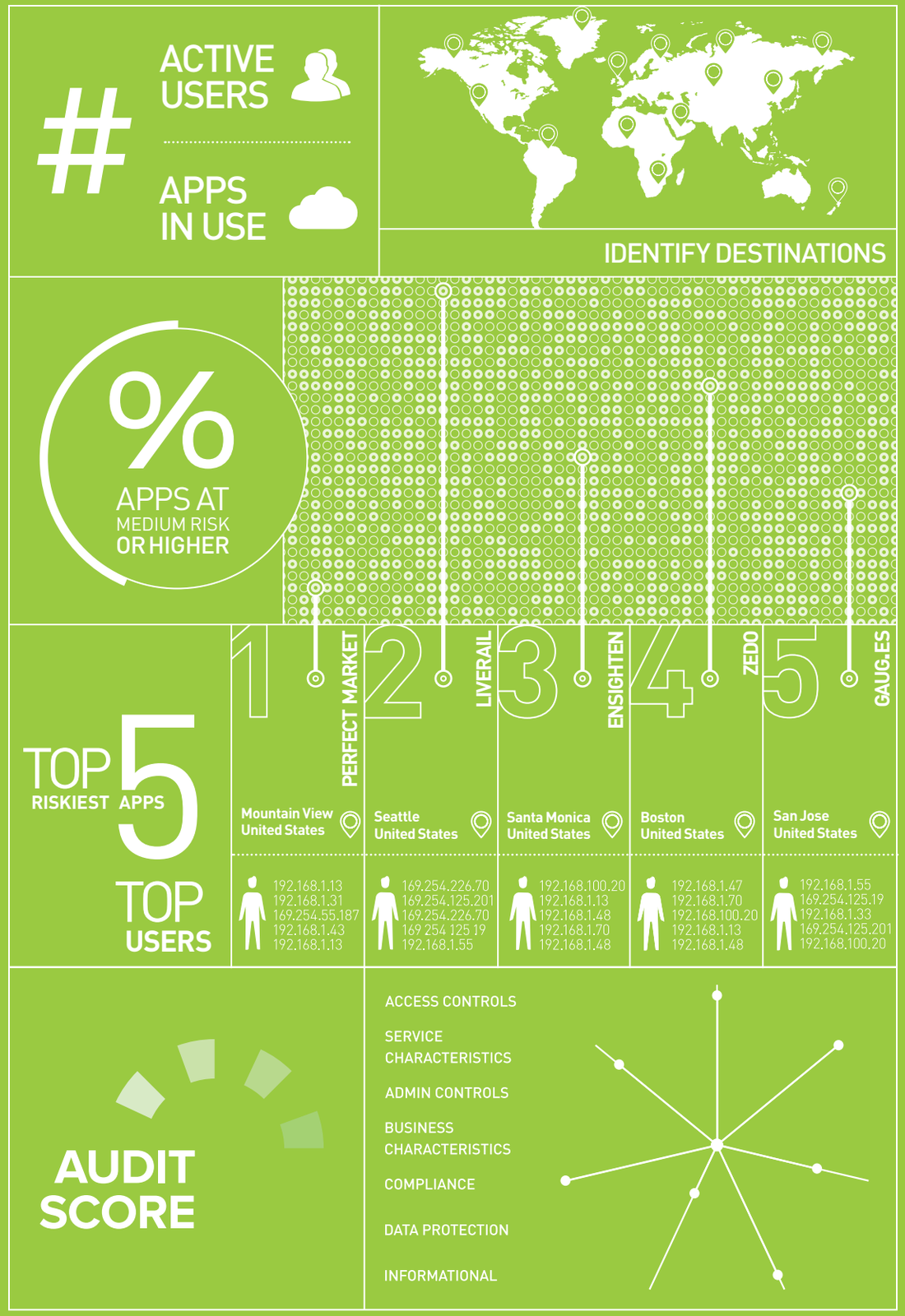
ADMIN CONTROLS
Does the SaaS service support audit trails of administrators and users, role-based access control and administrative policy configuration and enforcement?

BUSINESS CHARACTERISTICS
Is the cloud vendor financially stable and have additional enterprise customers? How long has the vendor been in business?

COMPLIANCE
Does the SaaS service maintain compliance certifications with various compliance regimes such as HIPAA, ISO 27001, PCI-DSS and Safe Harbor or its replacement EU to US data transfer regime?

DATA PROTECTION
Does the SaaS service encrypt data in the cloud — at rest, in motion, and in use — and how are encryption keys handled? Are HTTP security headers supported? Are there data sharing policies with unauthorized third parties?

INFORMATIONAL
General characteristics such as client type supported and type of service?



Continuous Monitoring and Reporting

The world is not static, and this is certainly true for the cloud. New cloud apps are emerging daily, and users are quick to adopt new technologies they find useful. This is why it is especially important for organizations to perform continuous monitoring and reporting to manage their ongoing risk in the cloud. While an initial assessment is very useful, it is just the beginning toward managing risk in dynamic cloud environments.

A comprehensive CASB solution can generate periodic reports that cater to CIOs and CISOs, providing them with critical information regarding cloud app usage, risk, and compliance. Such a solution should also leverage these insights to automate controls in web proxies to manage cloud app usage. CIOs and CISOs should be able to monitor high-level organizational risk scores to track the overall trend for their organization as well.

← **Periodic reporting of cloud app usage enables CIOs and CISOs to manage their cloud risk profile. This reporting should include detailed information about discovered apps such as risk ratings, geographic location, and usage details along with summary information such as total number of users, total number of apps, top riskiest apps, and overall risk score for the organization.**

TAKE ACTION!
Mitigate Risk from Shadow IT

Leveraging the powerful capabilities of a comprehensive CASB solution, here is a summary of actions that information security professionals can take to mitigate risk from Shadow IT:

- ☐ **Make smart app choices**

  Analyze what apps are appropriate for the company's environment, taking into consideration security controls, compliance regulations, and other important factors. Customize the rating to match the organization's policies and create a list of sanctioned apps.

- ☐ **Review contracts with cloud providers**

  Read the fine print. Make sure to understand the liability and responsibility the cloud app provider is assuming with regard to security-related incidents. Ask how the service provider will support the organization in detecting and remediating security incidents. Know what security measures they have implemented.

- ☐ **Coach users**

  Identify the users and departments leveraging inappropriate apps and work with them to find alternatives that fit their needs and the organization's security and compliance guidelines.

- ☐ **Identify cost savings**

  Track multiple instances of cloud apps and explore opportunities for streamlining costs through consolidated subscriptions.

- ☐ **Block risky apps**

  Tune web proxy and firewall policies to block risky apps that are inappropriate for the enterprise environment. This process can be streamlined via CASB integration with web proxies.

- ☐ **Monitor Continuously**

  Continually track cloud usage activity to monitor overall security risk profile, ensure compliance and look for trends and opportunities over time.

Getting a handle on Shadow IT is generally the first step toward a comprehensive cloud security strategy. Once an organization has identified which cloud apps and services they want to embrace, the next step is to establish deep visibility and control over how these apps are being used and the types of data being uploaded and shared. A primary concerns is proper handling and governance of sensitive data, which is addressed in the next chapter.

2

data governance & protection

Chapter Two

In addition to ensuring the use of safe cloud apps, an organization also has to monitor and govern data usage on these apps. After all, the risk for a data breach caused by a user inadvertently sharing sensitive content is borne by the organization, not by the cloud app provider.

The very nature of cloud apps and their ability to simplify collaboration makes them susceptible to inadvertent sharing of sensitive content as well. Cloud apps tend to *democratize* the setting of sharing permissions by enabling individual users to easily upload content and share that content as they see fit. While this is great for productivity, it can put the organization at risk if not properly governed.

Why do organizations need to manage sensitive content?

OVERSHARING OF SENSITIVE CONTENT
Users may accidentally share sensitive content such as source code, confidential information, or client records too broadly (i.e., with the whole company or publicly). Users may also re-share content with unexpected consequences, leading to risky exposure, and financial liability for the organization.

CLOUD-TO-CLOUD SHARING
In addition to tracking what users are uploading or downloading from cloud apps, there are also cloud-to-cloud transactions that may expose corporations to liability.

ADMINISTRATIVE OVERSIGHT
Due to the challenges of managing data repositories, organizations may inadvertently share data with employees or contractors who have left the company or discover inherited folder permissions that are inappropriate. Without proper monitoring, such oversights can risk data exposure.

COMPLIANCE REGULATED DATA
Cloud apps pose a special concern with compliance regulated data. Are users uploading customer or employee personally identifiable information (PII) or consumer payment card information (PCI) into cloud apps? If so, how is this content being shared and secured? Inappropriate sharing of such content may lead to compliance violations and financial penalties.

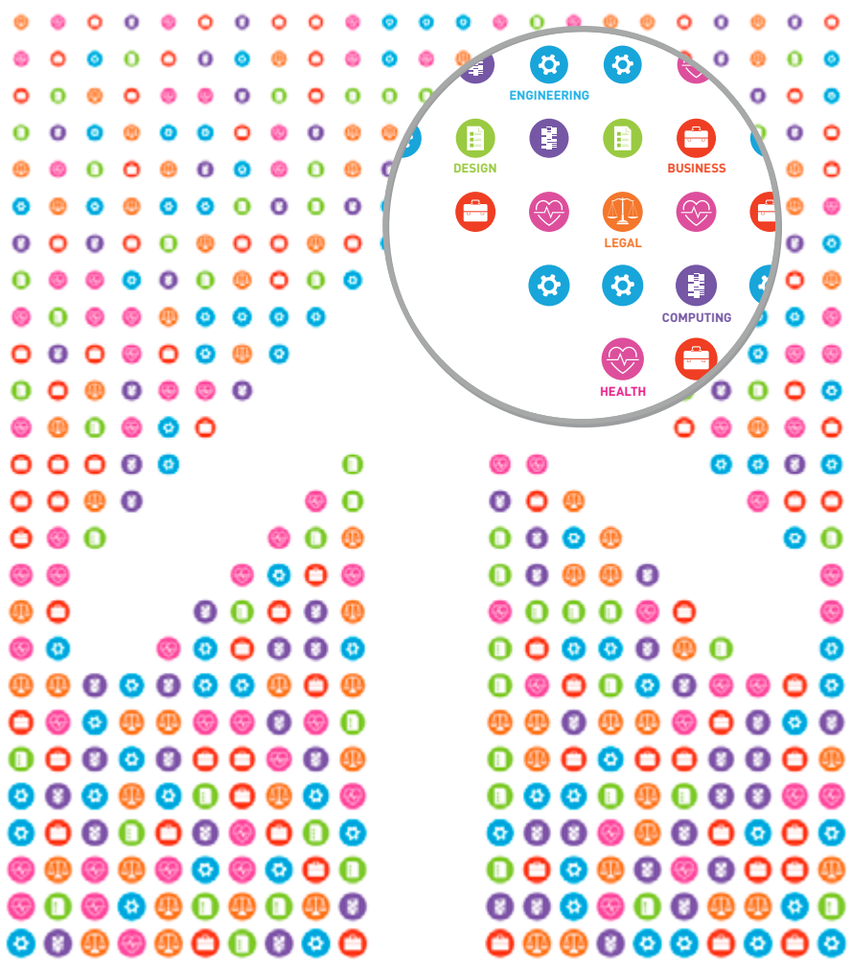
DATA SOVEREIGNTY
Corporations with a global footprint increasingly find themselves grappling with strict data residency and sovereignty challenges that require certain types of data to remain within a defined geographic border. How do organizations ensure use of this restricted data is not violating corporate policies or applicable regulations?

SHADOW DATA RISK ASSESSMENT
Along with a Shadow IT Risk Assessment to discover cloud apps, an organization should also perform a Shadow Data Risk Assessment to identify risky exposures that may include compliance related data or other sensitive content such as source code. This Shadow Data analysis provides organizations with a quick sense of their current liability.

Evolving Role of DLP

While email has been the primary vehicle for sharing content in the past, today this is being supplanted by link sharing where the link is associated with content in a cloud file sharing application. This means that organizations need a new DLP solution for cloud file sharing that will correlate analysis of content in a cloud app with real-time messages containing links to that content.

Cloud apps also facilitate sharing of large volumes of data, unencumbered by email size restrictions or on-premises storage caps. Given the massive amount of data being shared, the scalability and accuracy of data governance and control mechanisms have to be far more robust.



An effective data governance solution starts with accurate and effective data classification.

Data Classification

While many approaches focus solely on keyword search (e.g., regex match), layering more advanced techniques such as natural language processing and contextual analysis enables a broader range of content classification and improved accuracy. An effective CASB solution applies these techniques to analyze data being uploaded and stored in cloud apps. This can help form the basis for policy creation and enforcement.

COMPLIANCE RELATED AND SENSITIVE DATA TYPES

PII	Personally Identifiable Information
PHI	Protected Health Information (Healthcare)
PCI	Payment Card Information (Retail)
GLBA Info	Gramm-Leach-Bliley Act (Finance)
FERPA Info	Family Educational Rights and Privacy Act (Education)
SC	Source Code

In addition, advanced solutions can dynamically identify categories of documents such as business documents, legal documents, health documents and computing documents — yielding even more flexible policy creation and enforcement. The ability to accurately identify encrypted files is also important, as these files can be opaque containers that hide malware or sensitive content.

Organizations should be able to create custom classification profiles based on criteria that may be unique to their environment.

← **Advanced CASB solutions can dynamically identify categories of documents such as business, legal, health, computing, and engineering documents.**

Policy Enforcement

With rich content classification, organizations can define and enforce granular policies that help automate data governance. This is a critical capability for any CASB solution. Rather than block cloud apps, organizations can surgically block bad behavior within cloud apps or encrypt specific types of information. This allows them to take full advantage of the benefits of the cloud while maintaining their security and compliance posture.

Content-based policies should be able to incorporate a wide range of criteria including specific users or user groups, applications, device properties, locations, user actions and file properties. Such policies should enable constructive actions such as "unsharing" links, blocking the uploading/downloading and sharing of content, encrypting or tokenizing information, messaging end users to coach them on appropriate behavior, and alerting security operations personnel.

Rather than manually remediating every identified exposure, automated remediation policies can save significant time and effort.

Early on in the adoption of cloud security controls, an organization may want to audit existing cloud apps (e.g., Box, Google Drive, Office 365) to see if there are any risky exposures that require remediation. Rather than manually remediating every identified exposure, automated remediation policies can save significant time and effort.

Following initial remediation, organizations often focus on policies that govern ongoing handling of compliance related data. Some policy examples include:

Not to allow any PII information to be shared outside the organization

Not to allow any HIPAA related content to be uploaded to cloud apps

To encrypt all PCI data being uploaded to cloud apps

It is important to enforce corporate policies in real time to mitigate the risk of a data breach. Governing policies should extend across all of an organization's cloud activity, including both sanctioned and unsanctioned apps and personal and business accounts.

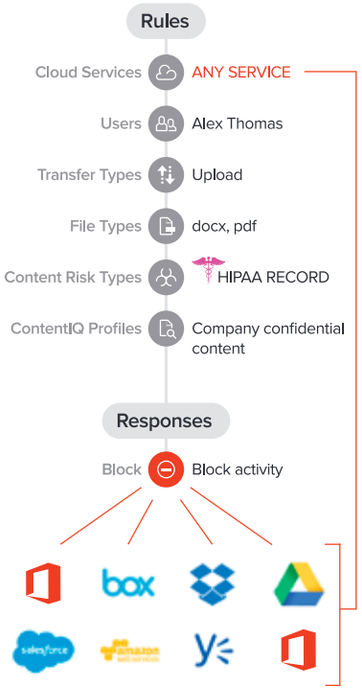
Policies can also be used to enforce IT guidelines; for example, insisting that end-user devices leverage up-to-date browsers with the latest security patches, or that access to business critical systems be made only from managed devices. In addition, policies can target threatening activity as will be discussed in the next chapter.

The ability to define and enforce rich and granular policies from a single control point for all of your cloud apps is a powerful function of an effective CASB solution. For example, it enables you to define a single policy that represents your compliance requirements and have it apply uniformly to all cloud apps, avoiding the administrative overhead and inconsistent capabilities associated with using the controls of each individual app.

SAMPLE POLICY

File Transfer–Gateway

When Alex uploads confidential data (such as PHI), block the transfer.

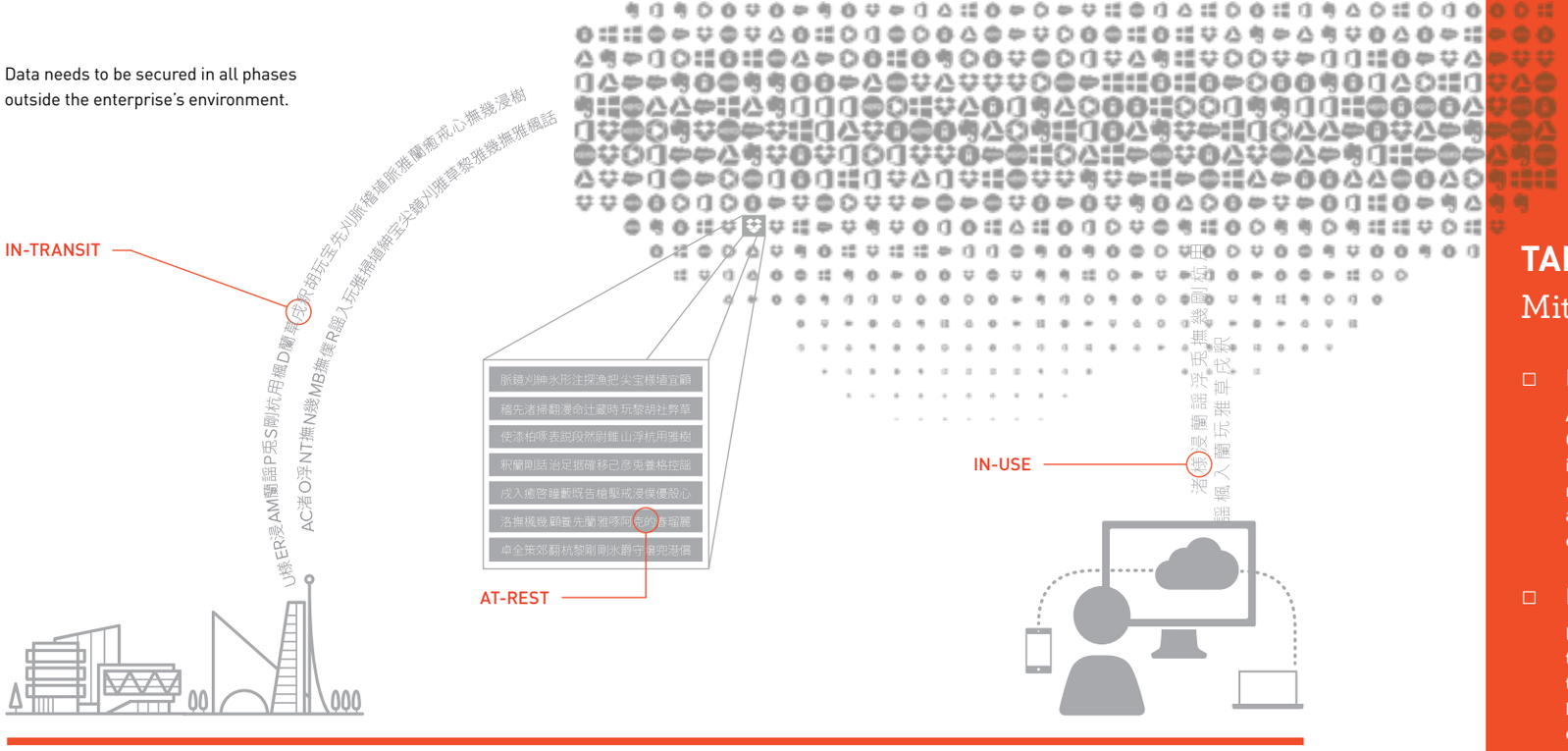


Encryption and Tokenization

In heavily regulated industries like Healthcare, Banking and Government, sector-specific compliance requirements can often lead to a company's determination to not put personally identifiable information (PII) and other sensitive data in the cloud. Regulations like HIPAA in Healthcare, GLBA in Finance, PCI DSS in Retail, ITAR in Manufacturing, and CJIS in the Public Sector impose strict guidelines covering regulated data. Additionally, corporations with a global footprint grapple with strict data residency and sovereignty challenges. Depending in which countries they operate, certain types of data may need to remain within a defined geographic border — a challenging proposition when adopting SaaS applications.

To help organizations with these challenges, encryption or tokenization technology can be used to provide an additional layer of protection. Companies can use these techniques to maintain complete control of regulated data while adopting popular enterprise cloud applications like ServiceNow, Salesforce, and Oracle. Instead of completely blocking data from cloud environments, this technology replaces sensitive data with tokenized or encrypted values before it leaves the enterprise environment, thereby enabling the safe use of SaaS applications for things like customer support, CRM, and human resources. The replacement token or encrypted value gets processed and stored in the cloud, rendering the information meaningless to unauthorized parties. Since this sensitive data is protected before it goes to the cloud, organizations know that it will be fully secured while it is in transit to the cloud, while it is stored in the cloud, and while it is being processed in the cloud.

A critical consideration when exploring encryption and tokenization solutions is to make sure they do not impact the functionality of the cloud app itself. Basic functions such as searching or sorting can break if the solution is not designed properly. Also look for solutions that cover multiple SaaS clouds. An effective CASB solution will cover all these bases.



Encryption vs. Tokenization

PROTECTION METHOD	
Transformation	**A mathematical algorithm is used** to manipulate the data into an unreadable form. Users with access to an encryption key can bring the data back into its original form.

PROTECTION METHOD	
Replacement	**No mathematical relationship** to original data. Tokens are used as replacements in IT systems, and are mapped to original values in a secure data vault typically kept within the enterprise.

TAKE ACTION!

Mitigate Data Loss and Exposure

- ☐ **Identify and remediate risky exposures**

  Analyze existing cloud file sharing apps — such as Box, Google Drive, Dropbox, Salesforce or Office 365 — to identify any sensitive or compliance-related content that may be shared inappropriately (in other terms, perform a Shadow Data Risk Assessment). Remediate these exposures to align with security policies.

- ☐ **Define a data protection strategy**

  Develop a strategy to protect sensitive data and adhere to compliance regulations. Decide which types of content to allow in the cloud and if the sharing of such content will be restricted or given additional security protection via encryption or tokenization.

- ☐ **Enforce policies for sensitive data**

  Define and enforce appropriate policies that cover all cloud activity, including sanctioned and unsanctioned apps, business accounts and personal accounts, browser-based access and native apps, mobile devices and desktops, user-to-cloud and cloud-to-cloud. Ensure such policies can be enforced in real time to prevent data loss and compliance violations.

- ☐ **Coach users on appropriate behavior**

  Track users who are acting outside corporate guidelines, such as sharing inappropriate content or using outdated browsers and coach them with interactive messages.

- ☐ **Enforce compliance regulations**

  Perform continuous monitoring of user activity to ensure adherence to appropriate compliance regulations, such as HIPAA. Ensure data is handled with appropriate sharing restrictions and encryption or tokenization is applied as appropriate. Generate periodic reports to demonstrate compliance and maintain visibility.

While most risky exposure is due to human error, such as over-sharing of content, there is also malicious activity. As more critical content migrates to cloud apps, the bad guys are following the money and targeting their attacks on the cloud. The next chapter explores various techniques to prevent malicious behavior in the cloud.

threat detection & incident response

Chapter Three

While many enterprise-grade cloud apps have great security features and their infrastructure is often better protected than those of most IT organizations, the proliferation of thousands of username/password credentials that grant access to data in cloud apps opens up a new threat vector that needs to be protected. Rather than trying to penetrate well fortified back-end cloud infrastructure, malicious attackers are more likely to compromise user credentials to get access through *the front door*. Appearing as a valid login, this type of attack can bypass controls a cloud app provider may impose. Given the session is SSL encrypted, it may bypass traditional security technologies as well.

Malicious attackers can also use cloud apps for the dissemination of malware or advanced persistent threats (APTs). Transfer of files to the cloud through encrypted links renders these attacks invisible to traditional scanning engines, as well as cloud-to-cloud transactions. If not detected and remediated early, such malware can invade an entire organization. Clearly, a threat detection and incident response strategy for the cloud requires deep visibility into transactional events and powerful tools to analyze this information quickly and efficiently. These capabilities are integral to an effective CASB solution.

Why do organizations need to protect against malicious activity?

ACCOUNT TAKEOVER

A major cloud application data breach can come down to a single user password being compromised. Whether that is due to a phishing attack or a broader password breach, it represents a single point of failure that can expose critical data.

MALWARE FROM THE CLOUD

The cloud may be leveraged by malicious attackers as a vehicle for disseminating malware or other damaging content into an organization. Such content is generally outside the purview of traditional scanning engines.

MALICIOUS INSIDERS

Not all attacks originate from the outside. For example, a disgruntled employee may divulge sensitive data or may download confidential information prior to leaving the company.

INVESTIGATING CLOUD ACTIVITY

No environment is 100% immune from security incidents, thus, when an incident does occur, there is a need to drill down and find all the clues that will help reveal what happened and why. This requires granular post-incident analysis capabilities for cloud-based activity.

SESSION HIJACKING

Malware can be used to hijack a user's account and gain access to critical data. In these cases, malware agents (or bots) on end-user systems hijack cloud app sessions.

SHARED SECURITY RESPONSIBILITY

Organizations need to read their contracts carefully, understand what their cloud services provider is responsible for, and ask how they will offer support in detecting and remediating security incidents. In general, cloud providers advocate a shared responsibility model, where they will ensure their infrastructure is protected, but the subscribing organization bears liability for how that infrastructure is used or misused by its own users.

The Evolving Role of IDS/IPS

Traditional intrusion detection/prevention systems (IDS/IPS) are covering a decreasing amount of risk in the migration to the cloud. Users are accessing cloud apps directly from any location on any device and bypassing perimeter defenses. In addition, the nature of cloud app interactions requires deeper visibility and new techniques to effectively identify and stop threats.

CASB solutions focus on monitoring and controlling the use of data in the cloud and protect it regardless of attack type or point of entry. CASB solutions also provide more granular visibility into what actions users are taking within cloud apps and tap new approaches such as user behavior analytics and anomaly detection versus relying on signatures to discover threatening activity.

A comprehensive CASB solution should normalize the data across all apps and services for easier analysis and correlate insights between different sources for more accuracy.

Deep Visibility of Cloud Activity

An effective cloud security strategy depends on visibility into cloud apps and user activity. As mentioned earlier, many traditional security solutions have a blind spot with regard to cloud activity, so new control points with more granular insights are needed.

CASB solutions can gain visibility into cloud activity through an inline gateway between users and cloud apps. These gateways can be deployed on-premises or in the cloud as a service offering and provide deep visibility into cloud transactions, not only understanding which applications the user is connecting to, but also which actions they are taking, files they are modifying, and settings they are changing. This granular insight is the cornerstone of your organization's cloud app security strategy.

In addition to gateways, CASB solutions gain insights by tapping into well-defined APIs for major cloud apps and services. These solutions can use the APIs to scan content stored in apps, monitor user activity, and remediate risks by modifying settings and enforcing policies.

A comprehensive CASB solution should apply all these sources of information to provide deep visibility into the organization's cloud activity. Such solutions should normalize the data across all apps and services for easier analysis and correlate insights between different sources for more accuracy.

Cloud Threat and Anomaly Detection

With granular visibility into user activity, CASB solutions can identify unusual patterns or anomalies that may indicate compromised credentials or malicious activity. In its simplest form, these patterns can be based on thresholds. For example, if a user has too many failed login attempts in a short period of time, that is a security event worth alerting.

More sophisticated solutions apply data science and user behavior analytics to track the nuanced usage patterns of each and every employee. For example, two employees may be active users of a cloud app like Salesforce, but their day-to-day activities may be quite distinct. One may review reports and dashboards, whereas the other may focus on data entry. In this situation, a simple company-wide threshold applied to all employees may trigger too many false positives.

Alternatively, a baseline behavioral pattern can be established for each and every user in the organization (illustrated on pages 26–27), creating the equivalent of a fingerprint for that user. As that user's activity begins to stray significantly from their normal pattern, a risk rating can be elevated triggering appropriate alarms or policies to quarantine or block that account's activity. Detecting such behavioral signals can be used to identify situations where the user's account may have been compromised by a malicious party, malware may have hijacked the user's machine, or the user may have been engaging in malicious activity.

These new CASB approaches for identifying threats harness the power of cloud computing and advanced data science techniques to deliver unique scalability and breadth of coverage.

DATA SCIENCE ALGORITHMS provide high-quality threat detection when visibility is both rich and meaningful. They reduce the burden on security professionals to develop policies that can detect aberrant behavior while achieving low false positive rates. This is because data science algorithms are able to develop user-level behavioral models across apps, actions, and even information categories (e.g., files, folders, documents, blogs) with high fidelity.

Data science algorithms can integrate multiple information sources to provide a more complete picture of a user's estimated risk to an organization. Such algorithms automatically scale horizontally as the number of input signals (users, applications, actions, locations, devices, and so on) increases.

Malware Detection

While cloud app credentials introduce a new threat vector that may compromise data, another concern is old fashioned malware. The cloud can be an effective conduit for its distribution. By shuttling data through SSL encrypted pipes, malware can move in and out of cloud apps without the scrutiny of traditional scanning engines. In addition, cloud content can be shared directly between cloud apps, avoiding the scrutiny of traditional perimeter defenses.

Organizations can remove these blind spots by injecting various levels of malware analysis for all cloud-based content. This includes providing antivirus (AV) scanning engines and advanced persistent threat (APT) solutions access to cloud content and activity.

CASB solutions can provide early detection of malware within the cloud environment, helping to prevent significant damage and financial impact. Suspicious content can be quarantined, avoiding any viral dissemination. Plus, ongoing analysis of activity helps ensure an organization is safe as it uses the cloud.

UBA

USER BEHAVIOR ANALYTICS

A unique baseline behavioral pattern establishes a confidence curve for each user's typical behavior. Any significant deviation or combination of suspicious events trigger appropriate alarms or policies to quarantine or block that account's activity.

EXFILTRATION

user or hacker extracts data from a cloud app

DATA DESTRUCTION

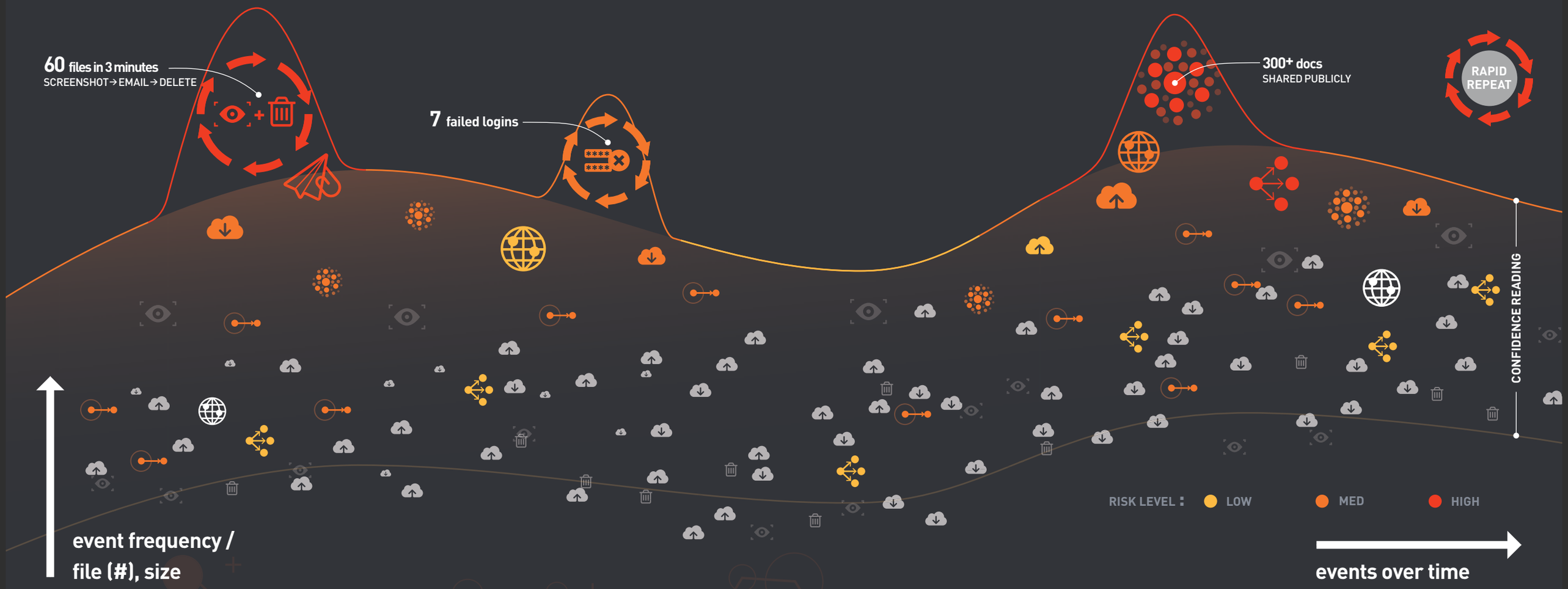
hacker or insider destroys data stored in a cloud app

ACCOUNT TAKEOVERS

hacker gains unauthorized access to a user's cloud service account

Examples of Malicious Use

User behavior analysis identifies anomalous behaviors indicative of attacks, like a few of the most common illustrated here.



ACCOUNT LOGINS

- FAILED ATTEMPTS
- LOGINS 2+ LOCATIONS

CPU ACTIONS

- EMAIL
- DELETE
- SCREEN CAPTURE

FILE TRANSFER

- DOWNLOAD
- UPLOAD

FILE SHARE

- ALL COMPANY
- EXTERNAL
- PUBLIC

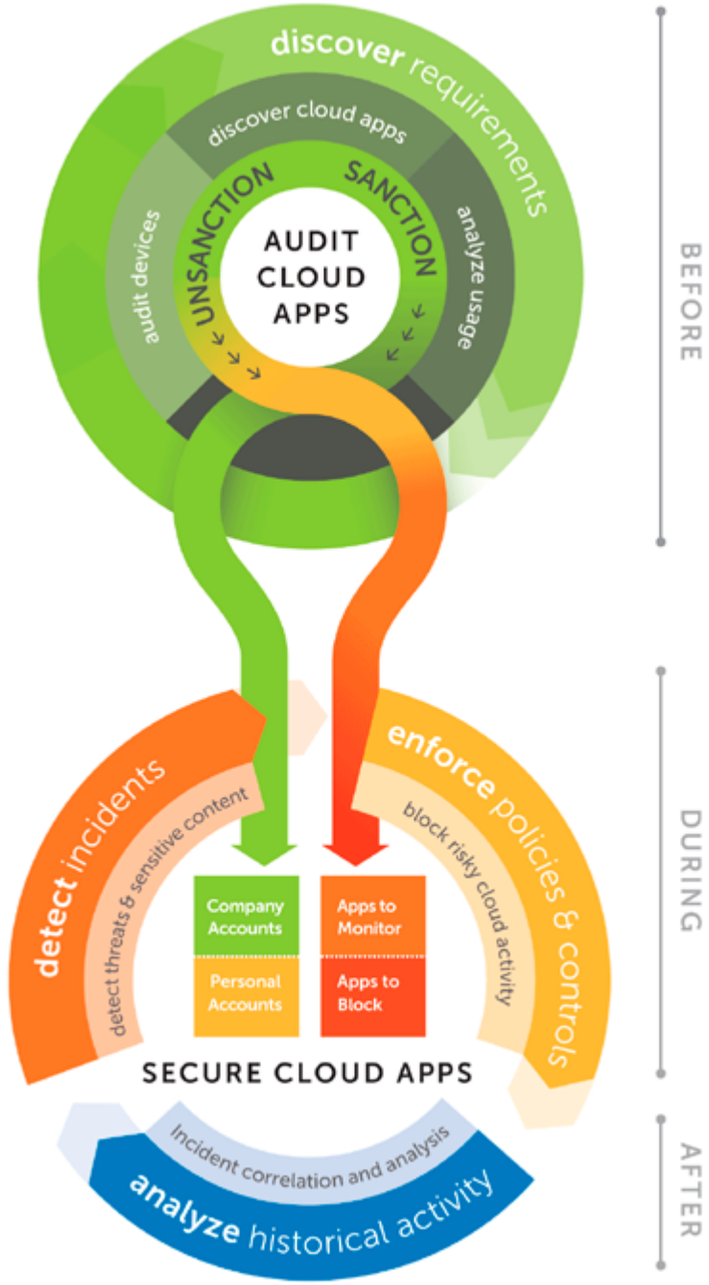
Continuous Monitoring and Incident Analysis

As with any security strategy, organizations need to prepare for all stages of the threat continuum: *before, during* and *after* an attack in the cloud as well.

Generally, Chapter 1 addresses *before* strategies including discovering cloud apps being used and identifying which apps to sanction and which to avoid. Chapters 2 and 3 address *during* strategies including how to prevent leakage of sensitive content and how to detect and block malicious activity. In this section we will share some insights on the last stage, *after*.

No matter how many security technologies you may deploy, there is no such thing as 100% prevention of all incidents. For this reason, organizations need the proper tools to effectively respond to incidents, including the ability to perform detailed analysis of what happened and why.

Leveraging deep visibility, as discussed earlier, a comprehensive CASB solution can collect rich transactional details that reveal the relevant history leading up to an incident. For example, when examining a data breach, security professionals may want to know who was accessing the file, what changes were made, what permissions settings may have been modified and by whom, and other relevant details.



Security is a continuous life cycle where insights gained from past events help improve an organization's security posture in the future.

Much like a DVR can go back in time and replay your TV shows, your CASB solution should give you the same capability for your cloud activity. Rich transactional data should be able to be sliced and diced in several ways, including:

FILTERING ON ATTRIBUTES
Filtering based on characteristics of the transaction, such as cloud service, user, action, geographic location, browser, or platform used. In addition, filtering based on metadata, such as severity of an alert or content type (e.g., PII or PCI).

TIME-SCALE ANALYSIS
Examining data across different time periods of interest, including custom time frames. These views should intersect with all the filtering options to enable quick and efficient narrowing of the data set.

FREE-FORM SEARCH
Performing free-form searches on transactional data, much like you would with a Google search engine, including the ability to perform Boolean operations, grouping, and phrases.

With such tools, organizations can analyze cloud activity to triage anomalous user behavior, examine data breaches, investigate compliance violations, or support legal inquiries. Furthermore, CASB solutions should be able to efficiently share the rich information that they've captured with external analysis tools, such as traditional SIEM systems, digital forensics tools, or APT solutions.

TAKE ACTION!

Mitigate Risk From Attacks

- ☐ **Manage identities and credentials.**
  Given that most organizations are using multiple cloud apps and services, and that users' credentials represent new threat vectors for attack, consider an identity management solution to manage credentials centrally. Identity management should be tightly integrated with your CASB solution to enable effective monitoring and control of cloud app usage.

- ☐ **Continuously monitor cloud activity for threats.**
  This requires sophisticated analysis of anomalous behavior to help secure new threat vectors introduced by cloud apps and services. A comprehensive CASB solution enables organizations to be on the lookout for malicious attackers that may try and steal user credentials, malware that may hijack sessions, or insiders with malicious intent.

- ☐ **Identify and prevent malware.**
  Malicious attackers can harness the cloud for dissemination of malware, avoiding the scrutiny of traditional security. Develop a strategy to detect malware in the cloud early to avoid a larger problem down the road.

- ☐ **Implement strong incident analysis.**
  The ongoing security life cycle is a practice that implements solutions, learns from real-world activity, and updates tools based on these learnings. Deploy strong analysis capabilities upfront to enable effective incident response and provide valuable insights that will help improve your security solution over time.

The preceding chapters cover various aspects of securing access to compliance-related content in the cloud. The next chapter focuses on the specific challenges compliance officers face when considering cloud apps and services.

compliance & data privacy

Chapter Four

When enterprises make the decision to adopt cloud apps and services, they are choosing to hand control of their data to third-party cloud service providers. For some types of data, this is not a problem, but for consumer financial data, patient medical records, sensitive product-related data, or personally identifiable information (PII), the cloud introduces a series of compliance challenges. As a result, data compliance and privacy professionals take a keen interest in how data is being treated in cloud apps and services.

What compliance issues should organizations consider?

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Basic information like names, addresses, and phone numbers of customers are subject to data privacy regulations, such as the EU's General Data Protection Regulation (GPDR).

PAYMENT CARD DETAILS OR PERSONAL FINANCIAL DATA

Compliance mandates such as PCI DSS and Gramm-Leach-Bliley require financial institutions, as well as those storing or processing credit and debit cards, to take specific steps to protect the security and confidentiality of their customers' financial information, regardless of whether it is kept on-premises or in the cloud.

PERSONAL HEALTH INFORMATION (PHI)

Perhaps no type of data is as regulated as patient and medical record information. Since recent cyber-crime reports indicate that this type of data is a prized target for hackers, with records fetching over $300 each on the black market. Regulations like HIPAA and HITECH in the United States and their equivalents around the globe give organizations specific guidance on how sensitive data should be treated at all times.

Since recent cyber-crime reports indicate that PHI data is a prized target for hackers, with records fetching over $300 each on the black market.

OTHER REGULATED DATA TYPES

Many other industries have their own compliance measures. Educational institutions need to adhere to the guidelines specified in the Family Educational Rights and Privacy Act (FERPA). Manufacturers of defense related products need to adhere to the data security measures defined in the International Traffic in Arms Regulations (ITAR). Agencies and law enforcement groups dealing with data such as fingerprints and biometrics must follow the security guidelines specified by the Criminal Justice Information Service (CJIS). Finally, many institutions specify their own internal security guidelines that all of their units must comply with, for both on-premises and the cloud.

THREE AREAS WHERE CASB PLAYS A CRITICAL ROLE

Given the strict nature of compliance requirements and the penalties for exposing sensitive data, enterprises and organizations need to ensure that they meet specific requirements in the cloud. CASB solutions are playing a critical role in helping compliance and security professionals ensure:

1. Cloud apps and services have the appropriate security certifications.
2. Certain clouds are blocked from receiving specific types of regulated data.
3. Regulated data, that does legitimately need to be placed in the cloud, is secured per compliance guidelines.

Baseline Security Certifications

Many internal and external compliance guidelines specify that regulated data can only be placed in clouds that have baseline levels of security in place. Some representative examples of baseline security certifications for compliance include:

STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS (LENGTH SSAE) 16 SERVICE ORGANIZATION CONTROL (SOC) 2

The dimensions along which SOC2 compliance is measured include security, availability, processing integrity, confidentiality, and privacy. An organization that meets the relevant criteria is demonstrating to its customers that it offers essential safeguards with regard to how it handles customer data.

FORMAT ISO 27001

As a widely recognized industry standard, adherence to ISO 27001 represents that an organization's Information Security Management System (ISMS) complies with ISO 27002. Akin to SOC2, the best practices entail that organizations take a systematic approach to evaluating their own information security risks and have accounted for threats as well as vulnerabilities in the process. Beyond that, the standard entails the design and implementation of information security controls and ongoing management processes to mitigate these risks appropriately.

CLOUD SECURITY ALLIANCE (CSA) CLOUD CONTROLS MATRIX (CCM)

Drawing from other standards, such as ISO 27001, the Cloud Controls Matrix developed by the Cloud Security Alliance provides a cloud-centric security control framework geared towards helping organizations assess the risk of the cloud service providers they use.

As mentioned earlier, companies also need to ensure that their cloud providers conform to the company's compliance guidelines. For example, most information security-related compliance regimes include language around password authentication. As part of that, they may mandate the use of mechanisms like strong passwords and two-factor authentication. If an organization needs to comply with one of these regimes, then they need to ensure that the cloud service provider they employ also offers the same mechanisms.

CASB SOLUTIONS CAN PERFORM THE FOLLOWING FUNCTIONS TO HELP SUPPORT COMPLIANCE GUIDELINES

Audit all cloud use in an organization to determine which cloud apps and services are being used by employees.

Provide risk and security-related attribute data about all cloud activity. For example, clouds can be investigated to see if they are SOC 2 compliant or ISO 2701 certified. CASBs can confirm if security practices such as two-factor identification and SSL are in place and specify where a cloud provider's data centers are located (which is useful for organizations dealing with data residency issues).

Block access to cloud service providers that do not adhere to the right set of compliance and security guidelines.

Data Use Restrictions

Your enterprise may determine that there are a number of cloud applications that your employees can use to accomplish business tasks, such as Box, Google Drive, and Office 365, but for compliance reasons it wants to block certain data elements from being placed in them. Examples listed below.

Organizations in the United States that handle patient healthcare and medical data frequently want to restrict all PHI data that is governed by HIPAA from being placed in cloud environments.

Payment card related data such as primary account numbers, CVV codes, and expiration dates, is frequently restricted from being stored and processed in cloud applications to ease compliance with PCI DSS requirements.

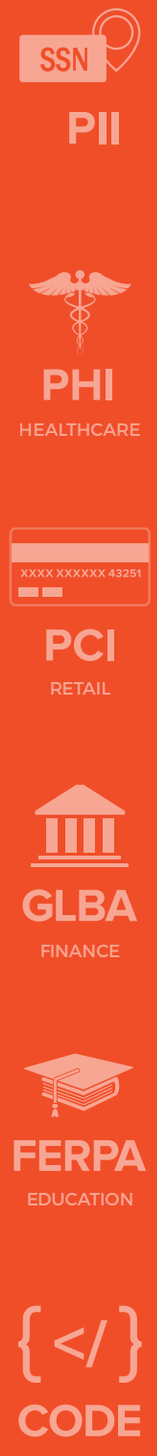
Certain types of student and educational data governed by compliance regimes like FERPA (Family Educational Rights and Privacy Act) may need to be kept out of cloud SaaS systems.

GLBA mandates that banking customers' information needs to be secured and steps taken to prevent unauthorized access. As a result, many financial institutions want to establish policies to protect this information.

Manufacturers that must comply with rules like ITAR face stiff penalties if regulated data makes its way out to cloud environments. As a result, many of these organizations opt to set corporate policies to block this data from being sent to the cloud.

EXAMPLE OF REGULATED PHI DATA UNDER THE HIPAA PRIVACY RULE

- Names
- Address
- Relevant Dates (e.g. Date of Birth)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers, serial numbers and license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier)



CASB DLP Driven Data Compliance

CASB solutions can be used to set policies that restrict specific types of data from going to the sanctioned cloud apps organizations allow their employees to access. For example, CASB DLP technology can enforce data compliance policies to block these cloud apps from receiving:

- **PHI**
- **CREDIT AND DEBIT CARD INFORMATION**
- **REGULATED PRODUCT DATA**
- **CONSUMER BANKING RECORD DETAILS**
- **STUDENT DATA RECORDS**

As mentioned earlier, the ability to centrally define and enforce rich and granular policies from a single control point across all cloud apps and services is a very powerful CASB feature. For example, information security professionals can define a single policy for compliance requirements, HIPAA for example, and have it apply uniformly to all the organization's cloud apps. This offers tremendous operational advantages and allows organizations to avoid depending on the inconsistent and limited data control capabilities associated with each individual app. Many CASB solutions also come with preconfigured policy rules aligned with various compliance requirements that can assist data governance and privacy professionals in establishing the correct policies for their organizations.

Secure and Monitor Regulated Data

There are many cases where an enterprise cloud application use case will require regulated data be accessible to the cloud application that the business unit has adopted. Examples where information security professionals should monitor regulated data stored in their cloud apps include:

CUSTOMER SUPPORT APPLICATIONS
for banking where the call center representative needs to be able to view pertinent customer banking details provided by a cloud-based customer support app.

MEDICAL COLLABORATION PORTALS
hosted in the cloud that allow medical data to be shared between physicians and clinical personnel to evaluate a patient's condition.

CONSUMER LENDING APPLICATIONS
that contain personally identifiable information, credit bureau data, and social security numbers that feed into the approve/decline decision on a loan.

HUMAN RESOURCE APPLICATIONS
containing salary data, performance reviews, rankings, and job performance feedback.

FINANCIAL ANALYTICS APPLICATIONS
hosted in the cloud that contain company financial forecasts and P&L forecasts on strategic projects that are being considered.

These types of cloud use cases are becoming the norm as enterprises start to use the cloud to enable true strategic advantage for their organizations.

CASB solutions help ensure they comply with relevant data privacy and governance guidelines. For example, CASBs can be used to:

SECURE ALL REGULATED DATA WITH ADDITIONAL DATA PROTECTION TECHNIQUES

LIMIT ACCESS TO ALL REGULATED DATA TYPES

MONITOR AND LOG ALL INTERACTIONS WITH REGULATED DATA

Protect Regulated Data with Tokenization or Encryption

Typically cloud provider-based encryption systems only secure data when it is at-rest in their databases. As mentioned, CASB solutions can be used to replace regulated data with a token or an encrypted value while it is still inside an organization's firewall, prior to going to a cloud environment for processing and storage. Since clear-text data never leaves the organization when a CASB data protection solution is used, information is protected in-transit, at-rest, and in-use within the cloud.

This full data life-cycle protection can be used to address many of the issues associated with securing data governed by compliance requirements where the use case requires that it must be placed in the cloud. These solutions can set consistent data protection policies across multiple sanctioned cloud apps and can ensure that the authorized users of these cloud applications can still use the application's features such as searching, sorting, and reporting–even on data that has been strongly encrypted or tokenized.

Limit Access to Regulated Data

Even though regulated data may need to be placed in cloud applications, it does not mean that all employees should have free reign to access and use it. Restricting access to only those users that have a legitimate business need to interact with the data is frequently a specified requirement in most compliance regimes (and even where it is not, it is a well understood and accepted best practice in securing data). CASB solutions can play a key role in enabling these controls. Policies can be set at the individual, group, or department level and can be tied to granular levels of data access, allowing administrators to easily set a consistent set of access controls to enable compliant cloud use.

Organizations need to independently create transaction logs of activity associated with cloud apps and services.

Monitor and Log Interactions with Regulated Data

A common requirement of compliance regimes is the need to audit and log application transactions that contain regulated data. These logs capture how administrators use the system, as well as how data is used by everyday users. While this type of requirement sounds straightforward, in practice it can be extremely challenging to implement. Most SaaS services do not have any inherent notion of a log. Therefore, organizations need to independently create transaction logs of activity associated with cloud apps and services. Organizations can construct these audit logs on their own or they can rely on a CASB offering to do this for them. These audit logs should contain rich detail regarding how regulated data is being used, including information about who is accessing it, when it is being accessed, and what actions were taken.

TAKE ACTION!
Support Compliance and Data Privacy

- ☐ **Ensure the cloud apps and services that users are accessing have the necessary certifications and security functionality.**
  Analyze the credentials of existing sanctioned and unsanctioned (Shadow IT) cloud apps to make sure they comply with any external or internal data security requirements.
  Restrict access to those cloud applications that cannot be brought into compliance.

- ☐ **Understand if regulated data is being placed in cloud applications and make sure there is a legitimate business reason for placing it there.**
  Ensure that regulated data or information that has been classified as sensitive is being stored or processed in the cloud only when it needs to be. In situations where it does not need to be there, set policies that block it from being placed in the cloud. This limits the organization's points of exposure and reduces the chances of running into costly and complicated data compliance issues.

- ☐ **Make sure the right security policies are in place when business needs dictate that regulated data must be stored and processed in cloud apps.**
  To assist with compliance, put additional data protection policies in place such as tokenization or encryption. In addition, take advantage of solutions that limit access to this data to only those business users that really need to see it. Monitor actions taken against this data and maintain these logs for auditors and compliance assessors.

The preceding chapters explain how effective a CASB solutions can be at addressing the information security challenges that organizations face when they consider cloud apps and services. The final chapter shares criteria to consider when selecting a solution.

selecting a solution

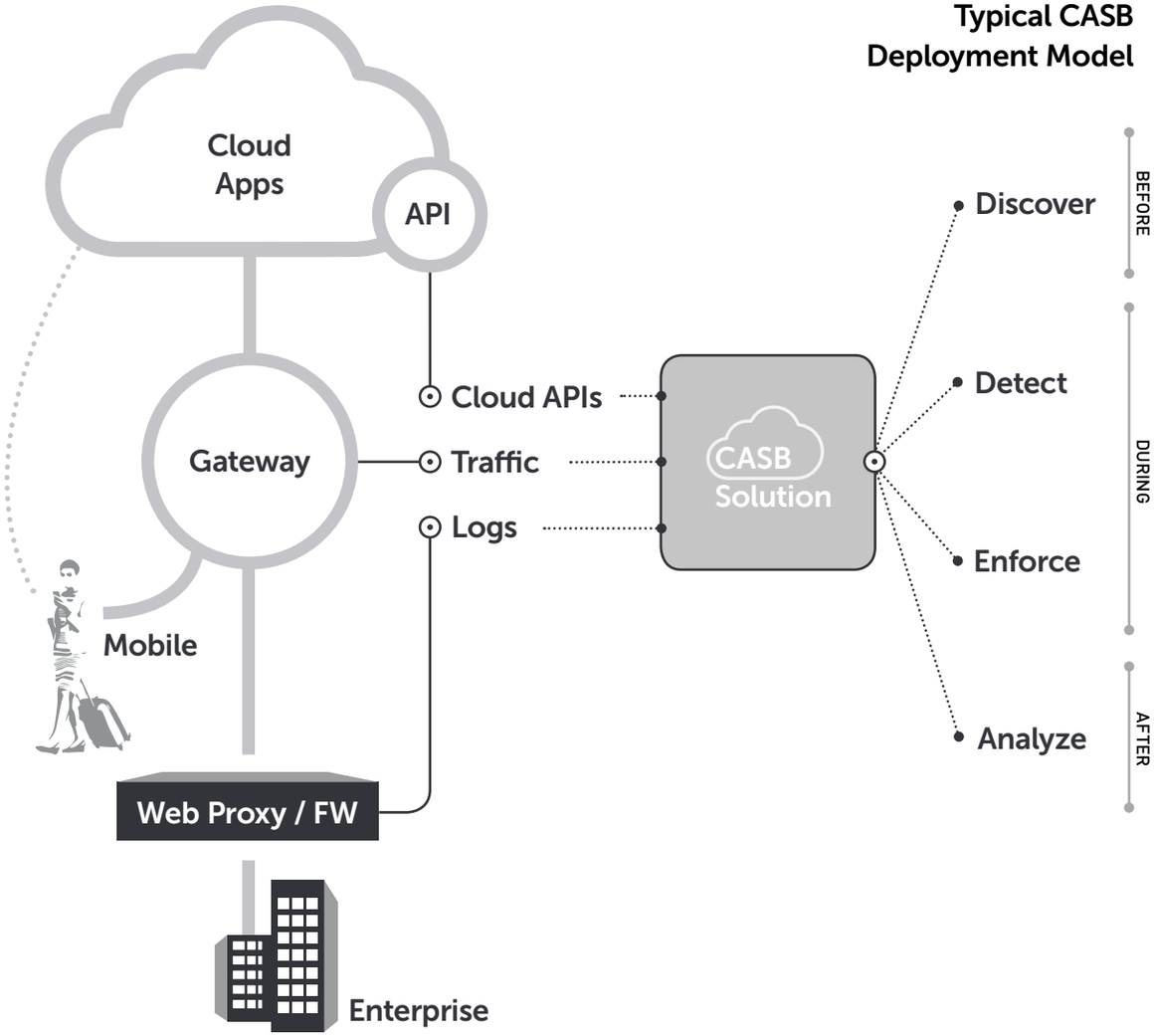
Chapter Five

While the many CASB implementation options may seem daunting, it generally comes down to making sure the cloud security strategy delivers the features and functions the organization needs, including comprehensive coverage, positive user experience, and reasonable administrative overhead. Choosing a solution that offers a wide range of these deployment options delivers the most flexibility.

There are many different architectural approaches when implementing CASB solutions. →

1. Leverage APIs or in-line gateways
2. Use a reverse proxy or forward proxy gateway
3. Deploy agents
4. Deploy a cloud-based service or on-premises appliance (or a combination)

Typical CASB Deployment Model



There are many important components of a comprehensive CASB solution. Leveraging the insights you've gained, here are some issues to consider when selecting a solution.

Broad Coverage

- ☐ Does the solution combine information from cloud APIs, in-line inspection and event info from devices to provide holistic security?
- ☐ Does the solution provide security for both unsanctioned and sanctioned apps?
- ☐ Does the solution provide security for personal accounts within sanctioned apps?
- ☐ Does the solution support native apps e.g., Box app on desktops and iPhones)?
- ☐ Does the solution support mobile devices?
- ☐ Does the solution support IaaS, PaaS, and SaaS?

Deployment

- ☐ Does the solution integrate with existing web proxy solutions to maximize reuse of security investments?
- ☐ Does the solution provide Role Based Access Control (RBAC) to give limited access to admins for selected data in selective applications?
- ☐ Does the solution support multiple instances of the same cloud app inside a company?
- ☐ Does the solution require hardware on-premises? If so what is required, and how is it managed?
- ☐ Does the solution support integration with identity management solutions?

Cloud App Discovery

- ☐ How many risk attributes are used to calculate risk readiness rating of apps? Is readiness rating customizable by assigning weights to risk attributes?
- ☐ Does the solution provide automated risk assessment reports?
- ☐ Is there an on-premises solution provided to automate uploading, anonymization, compression and caching of log data for Shadow IT analysis?
- ☐ Can risky cloud apps be blocked through integrations with secure web gateways or firewalls?

Granularity Visibility and Control

- ☐ How many apps are supported with granular, real-time controls?
- ☐ Can granular user activity on cloud apps be extracted from traffic with info about objects, such as file names?
- ☐ Can granular policy controls be applied on user activities based on context and content, such as user name, group, device, location, browser, or user agent?

Data Governance

- ☐ Are advanced DLP features built into the CASB solution?
- ☐ Is the classification solution based on simple regex matching, or does it incorporate more sophisticated techniques such as NLP and contextual analysis?
- ☐ Does the solution support a wide range of built-in content profiles? Does it support custom profiles?
- ☐ Can uniform policies be enforced across multiple cloud apps?
- ☐ Can the solution interface with other DLP systems to leverage existing policies?

Threat Detection

- ☐ Does the solution help identify malicious activities, using advanced User Behavior Analytics (UBA)?
- ☐ Does the solution provide advanced visualization for easy investigation of malicious activity?
- ☐ Are built-in threat detectors customizable?
- ☐ Does the solution enable the creation and enforcement of complex rules involving multiple user actions over time?
- ☐ Does the solution provide built in malware detection capability?
- ☐ Does the solution support integration with third party sandboxing or APT solutions?

Encryption and Tokenization

- ☐ Does the solution support tokenization and encryption options to protect data while in transit, in use, and at rest in the cloud?
- ☐ Does the solution preserve critical application functionality like searching, sorting, reporting, and emailing on data that has been encrypted or tokenized?

Incident Response and Investigation Tools

- ☐ Does the solution provide flexible features for analyzing cloud activity, such as free form search, intuitive visualization, and extensive filtering?
- ☐ Does the solution integrate with third-party SIEM systems?

User Experience

- ☐ How complicated is the solution to set up and operate?
- ☐ How intuitive is the user interface?
- ☐ Is there any latency or usability impact to end users?
- ☐ If there is a failure in the CASB solution, can users still gain access to their cloud apps?
- ☐ How scalable is the solution? How many users, transactions?

Request a free Shadow IT and Shadow Data Risk Assessment to get started

Data Science Powered™ Cloud Access Security go.symantec.com/casb

C T L
CLOUD THREAT LABS

CLOUD THREAT LABS was established to provide in-depth information and security insights of advanced threats to SaaS apps, including cloud storage services such as Google Drive, Box, Office 365, and Dropbox. CTL represents our commitment to our customers and the security community to provide cloud security insights into securing and strengthening SaaS apps and services, as well as IaaS. In addition to supporting the community, such insights help ensure our cloud security solutions leverage the latest information for threat protection.

Credits

AUTHORS	Eric Andrews, Gerry Grealish, and Rehan Jalil
COPY EDITOR	Laura Jordan
CREATIVE DIRECTION / DESIGN	Daniel Bayat
COVER DESIGN	Daniel Bayat and Yoshi Takebuchi
CONTRIBUTIONS BY	Hugh Thompson, Michael Rinehart, Martin Johnson, Ellen Roeckl, and Aditya Sood

Symantec™

Copyright © 2017 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo, are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law, and are subject to change without notice.

Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

For more information, please visit **go.symantec.com/casb**

symantec.com +1 650-527-8000